

# TAB I

UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF NEW HAMPSHIRE

* * * * *	*
	*
BETH ANNE M. COLLOPY	*
	* Civil Action
-vs-	* No. 1:22-CV-
	* 00184-SE
MARQUIS MANAGEMENT, LLC	*
	*
* * * * *	*

DEPOSITION OF IRVING SANTOS

Deposition taken by agreement of counsel using  
Zoom remote videoconferencing technology on Monday,  
June 26, 2023, commencing at 1:02 p.m. EST

Remote Court Reporter:

Lynda W. Eldred, LCR #43, RPR, RMR, CRR

1 mean by "cases" the same thing as tickets?

2 A. Yes, sir.

3 Q. Okay. And who'd she delegate her tickets or  
4 cases to?

5 A. The team.

6 Q. Okay. Well, wasn't she part of the team?

7 MS. ZACCARDELLI: Objection to form.

8 A. Yes. She was part of the team.

9 Q. BY MR. MEYER: How would you describe your  
10 work relationship with Ms. Collopy?

11 A. I -- I don't know.

12 Q. Now, you earlier referred to a ransomware  
13 attack.

14 Approximately when did that attack occur?

15 A. December 3rd of 2020.

16 Q. Do you have any prior experience in  
17 responding to ransomware attacks?

18 A. Yes, but not at this magnitude.

19 Q. And when you say "this magnitude," can you  
20 describe what you mean?

21 A. This was a very big and well-known attack  
22 that attacked many major businesses across the US, so  
23 at this caliber of attack, we had to pull in resources

1 to help us and those resources were Tracepoint.

2 Q. And -- and what is Tracepoint?

3 A. They are an cyber forensic consultant firm.

4 Q. Now, was there a -- you said this was a --  
5 sort of a national type of ransomware attack.

6 Did it have a name given to it?

7 A. Conti.

8 Q. Can you repeat that, please?

9 A. Conti, C-O-N- --

10 Q. Can you spell it, please?

11 A. C-O-N-T-I. Con- -- Conti Ransomware.

12 Q. Yeah. Sir, how did you become aware of this  
13 ransom attack?

14 A. I received a phone call 6:00 in the morning  
15 on Sunday from the individual that hosts our ERP  
16 system. He was stating that there was a lot of crazy  
17 -- I want to say high CPU usage, and when he relayed  
18 that message to me, I immediately went into all our --  
19 all my systems. I noticed the same -- when I say "all  
20 our systems," all the systems that are hosted within  
21 our building. I immediately went into those systems  
22 and I saw the same stuff that he was seeing on his end,  
23 and I immediately shut down all the systems and called

1 Chris Moore and informed him of what was happening  
2 and -- and continued to work with the individual that  
3 called me about the ransomware attack that was  
4 happening on his end.

5 Q. Was there a request for ransom made to  
6 Marquis, to your knowledge?

7 A. Yes, there was.

8 Q. And how long did it take to address the  
9 ransom -- the attack?

10 MS. ZACCARDELLI: Objection to form.

11 A. Can you repeat the question?

12 Q. BY MR. MEYER: Yes.

13 How long did it take to address the attack,  
14 to respond to it?

15 A. It took several months.

16 Q. Was there a certain point at which you felt  
17 that the scenario had been resolved?

18 A. Once we had the -- the tools that I needed  
19 in place, I felt that the ransomware was taken care of.

20 Q. And approximately when was that?

21 A. That was towards the end of January.

22 Q. And what was the nature of the response to  
23 the attack?

1 A. Can you repeat the question, sir?

2 Q. Yeah.

3 What did you do -- what did you and  
4 Tracepoint do in response to the attack?

5 A. We did a best practice in terms of roles  
6 within our IT department, so we had to remove some  
7 roles for the individuals that worked in the IT  
8 department. We had to ensure that back-ups weren't  
9 altered. We also had to store the infected systems for  
10 forensic, and to remediate, we had -- we implemented  
11 single sign-on for VPN connections.

12 Q. You said "remove some roles in the IT  
13 department."

14 What do you mean by that?

15 A. Some administration roles. Office 365  
16 platform.

17 Q. Does that mean you had to remove access for  
18 certain individuals in the IT department?

19 A. Yes.

20 Q. And what was the reason that you did that?

21 A. It was recommended by Tracepoint to do this  
22 as to -- to ease the -- the attack -- the surface --  
23 the attack surface from -- from the threat actor.

1 Q. Who decided which roles to remove?

2 A. I decided.

3 Q. Whose roles did you remove?

4 A. I removed Matt, Esdras, and Evgenii.

5 Q. Did you remove them all equally?

6 A. I removed them all equally.

7 Q. And how long between when you removed and  
8 when you restored them?

9 A. I'm sorry. Can you say that again?

10 Q. How long between when you removed them and  
11 when you restored them?

12 A. I can't recall.

13 Q. And did you restore them all at the same  
14 time?

15 A. I can't recall.

16 Q. Did Mr. Tanner have more access than the  
17 other IT individuals?

18 A. I believe he did.

19 Q. How was his access greater?

20 A. He was given exchange admin roles and  
21 in-tune roles.

22 Q. Did you have any conversations with  
23 Mr. Lieber about the access that was granted or denied

1 -- the -- the court reporter is going to read back your  
2 answer.

3 THE WITNESS: Oh, okay.

4 (The record was read as requested.)

5 MR. MEYER: Thank you.

6 Q. BY MR. MEYER: Sir, there's been testimony  
7 from other witnesses that in the approximate timeframe  
8 January 2021, you received a written warning.

9 Do you have a recollection of that?

10 A. Yes.

11 Q. Okay. And tell me, what -- what were you  
12 warned about?

13 A. I was warned to do things out of my role.

14 Q. And had you done things out of your role?

15 A. In that incident, yes.

16 Q. Okay. What is it you had done outside of  
17 your role?

18 A. I was monitoring the IT department's  
19 activities.

20 Q. Now, when you say "monitoring the IT  
21 department's activities," were you monitoring  
22 everybody's activities or activities just of certain  
23 members of the IT department?

1           A.     The help desk team.

2           Q.     You were monitoring the entire help desk  
3 team?

4           A.     Yes.

5           Q.     Okay. And what was the reason that you were  
6 monitoring the entire help desk team?

7           A.     Given that they have administration roles,  
8 I -- I took it upon myself to monitor them and make  
9 sure that during the ransomware remediation process  
10 that there wasn't anything suspicious going on on their  
11 system.

12          Q.     Now, did you detect anything suspicious  
13 going on on anybody's system?

14          A.     Yes.

15          Q.     What did you detect?

16          A.     I detected copies, extractions of files,  
17 external sources being mounted on a system, files being  
18 loaded to them. This rang bells and I -- and I saw  
19 them.

20          Q.     So -- now, was this by one person or by  
21 multiple people?

22          A.     This was by one person.

23          Q.     And who was that one person?

1           A.     Beth Anne.

2           Q.     Okay. And in terms of those observations,  
3 what follow-up, if any, did you do?

4           A.     I -- I -- I looked into the matter and I  
5 didn't -- was looking to see -- I -- I was looking to  
6 see if there was anything else.

7           Q.     Did you find anything else?

8           A.     The only thing I saw was data being  
9 extracted.

10          Q.     Now, did you discuss that with Ms. Collopy?

11          A.     No.

12          Q.     Did you discuss that with Mr. Moore?

13          A.     Yes.

14          Q.     Okay. Tell me what you can recall of your  
15 discussion with Mr. Moore.

16          A.     I told Moore -- Mr. Moore that I was  
17 monitoring the IT department and I noticed that there  
18 was extractions of data -- coming-in data going into an  
19 external source.

20          Q.     And what did he say?

21          A.     He was upset. He said that I should not  
22 have done that without checking with him first.

23          Q.     But did he do anything in terms of saying

1     what you should do about this extraction?

2             A.     I was given a warning.

3             Q.     No.    You were given a warning, but did he  
4     tell you what to do in terms of -- was there  
5     anything -- in terms of this -- this sent -- this --  
6     you said extraction from an external source.

7                     What was the external source?

8             A.     It was a drive of some sort mounted on the  
9     machine.

10            Q.     And was there anything -- in terms of doing  
11    that, was there anything that Ms. Collopy was doing  
12    that was improper?

13            A.     I was just monitoring activities on her  
14    machine, sir.

15            Q.     I know, but in your opinion -- you may not  
16    have one but if you have an opinion, was she doing  
17    anything that was violating Marquis rules or  
18    procedures?

19            A.     It -- it looked like that, yes.

20            Q.     Okay.    So was anything done to further  
21    investigate?

22            A.     I just reported it to my higher ups.

23            Q.     And that was Mr. Moore?

1 Q. BY MR. MEYER: Yes.

2 Did Ms. Collopy ever take on the role of  
3 assigning to other members of the help desk the tickets  
4 to be done?

5 A. Yes, she had -- she had delegated some  
6 requests.

7 Q. So she delegated tickets to other  
8 individuals?

9 A. Yes.

10 Q. And was that anything you discussed with  
11 her?

12 A. No.

13 Q. Did Mr. Moore ever advise you that an  
14 investigation was being performed of complaints made by  
15 Ms. Collopy?

16 A. I can't recall.

17 Q. Did you ever make any complaints to  
18 Mr. Moore about Ms. Collopy?

19 A. I can't recall.

20 Q. Did you ever have any discussions with  
21 Mr. Watkins about Ms. Collopy? And I say  
22 "discussions." I mean either oral or written.

23 A. I can't recall.

1           A.     That -- I can't recall what -- exactly what  
2     -- what was the substance.

3           Q.     Well, did he tell you that Ms. Collopy was  
4     unhappy because she felt that her messages had been  
5     deleted from teams?

6           A.     Yeah. I believe -- I believe he did.

7           Q.     And is it true that Ms. Collopy's messages  
8     on teams were specifically targeted for deletion?

9           MS. ZACCARDELLI: Objection to form.

10          A.     Based on the suspicion I saw, I thought it  
11     was in -- I was in my right to remove a set of  
12     policy -- sorry. -- set a policy in her teams chat.

13          Q.     So was this 15-day deletion only applicable  
14     to her teams chat?

15          A.     Yes.

16          Q.     And what was the connection between doing  
17     that versus the ransomware attack, if any connection?

18          A.     Well, there was a bunch of screen shots  
19     happening off from a teams chat. I'm not sure why that  
20     activity would be happening on her machine, so I  
21     responded swiftly by setting the policy.

22          MR. MEYER: Again, I think there was a -- on  
23     mine, I couldn't hear part of what he said.

1                   Could you read his answer back, please,  
2   Lynda.

3                   (The record was read as requested.)

4           Q.     BY MR. MEYER:  When you say "screen shots on  
5   her team chat," can you explain what you mean by that?

6           A.     Well, there was a lot of content that was  
7   being copied from that chat or chats that she had, and  
8   they were being stored external.

9           Q.     But did you report that to anybody?

10          A.     No.

11          Q.     I guess what I -- you -- you I think earlier  
12   indicated you thought that was suspicious; correct?

13          A.     Yes.  And so . . .

14          Q.     But my question is:  If there was suspicious  
15   activity going on on her teams chat in the immediate  
16   aftermath of this massive ransomware attack --

17                   THE COURT REPORTER:  Everybody froze.  
18   Hello?

19          A.     -- the case but to have already --

20                   THE COURT REPORTER:  I'm sorry.  It  
21   completely froze on me --

22          A.     -- being bombarded with a lot of tasks all  
23   over the place and I needed to --